Please amend Claim 8, 15 and 24 as follows:

8. (Once Amended) A method for providing certificate updates, the method comprises the steps of:

a) generating, by an end user, certificate update subscription information that includes at least identity of a plurality of subscriber subjects that the end user is interested in and their associated public keys, and receiving the certificate update subscription information from the user, wherein the certificate update subscription information includes current certificates for those subscriber subjects that the end user has a desire to communicate with, at least one of identity of at least one of subscriber subject, a public key certificate of the at least one subscriber subject, an attribute certificate of the subscriber subject, identity of a certification authority and a cross-certificate;

b) monitoring certificate of the at least one subscriber subject;

c) when a change occurs to the certificate, providing an indication of the change to the user,

the method further comprising receiving an indication of a user replica of the certificate from the user, when the use is on-line;

determining whether the user replica of the certificate is consistent with server replica of the certificate; and

when the user replica of the certificate is inconsistent with the server replica of the certificate, providing an indication of the server replica of the certificate to the user.

15. (Once Amended) A method for obtaining public key certificate updates, the method comprises the steps of:

a) generating by a user, certificate update subscription information that includes at least identity of at least one subscriber subject that the end user is interested in and their associated public keys, and providing by the user, the public key certificate update subscription information to a server, wherein the public key certificate update subscription information

identifies at least one subscriber subject that the end user is interested in and their associated public keys;

b) monitoring, by the server, public key certificate of the at least one subscriber subject;

c) when a change occurs to the public key certificate, providing, by the server, an indication of the change to the user;

d) while on-line, receiving, by the user, the indication of the change; and

e) determining, by the user, newly updated public key certificate based on the indication of the change.

24. (Once Amended) A server of secure communication system, wherein the server comprises:

processing unit;

memory operably coupled to the processing unit, wherein the memory stores programming instructions that, when read by the processing unit, causes the processing unit to (a) generate by a user certificate update subscription information that includes at least identity of at least one subscriber subject that the end user is interested in and their associated public keys, and receive the certificate update subscription information from the user, wherein the certificate update subscription information for those subscriber subjects that the end-user has a desire to communicate with includes at least one of: identity of at least one of subscriber subject, a public key certificate of the at least one subscriber subject, an attribute certificate of the subscriber subject, identity of a certification authority and a cross-certificate; (b) monitor certificate of the at least one subscriber subject and the certification authority;(c) provide an indication of a change to the user when the change occurs to the certificate; and

(i) receive an indication of a user replica of the certificate from the user, when the user is on-line; (ii) determine whether the user replica of the certificate is consistent with server replica of the certificate; and (iii) provide an indication of the server replica of the

certificate to the use when the user replica of the certificate is inconsistent with the server replica of the certificate.